PETTY CASH, ADVANCE ACCOUNT

Risks
- Use of petty cash for private purposes
- Submission of fraudulent petty cash claims
- Theft of cash

Causes
- Claims not adequately reviewed by supervisors
- Payment of claims without authorisation
- Payment of claims without receipts
- Advance accounts not regularly reconciled by independent officers
- Petty cash claims and receipts not stamped as 'paid' following reimbursement
- Nature or volume of purchases not shown on claims
- Large volume of small transactions
- Poor security of cash holdings
- Excessive cash kept on hand

Prevention Measures
- Petty cash approval closely reviewed and suspect items challenged
- All cheques signed by two independent officers
- Claim payments properly acquitted to avoid multiple payments
- Complete details of expenditure involved including receipts
- Adequate security of cash holdings including limiting access to safe, procedures re. regular banking etc.
- Quarterly and random audits

MATERIALS, TOOLS AND EQUIPMENT

Risks
- Materials, tools and equipment used for private purposes
- Theft of materials, tools and equipment

Causes
- Inadequate stock-takes
- Inadequate asset registers
- Poor physical security
- Poor records of movement
- Poor controls over purchase and issue
- No accountability for usage
- No serialisation of equipment
- No records maintained of material usage for jobs
- Poor awareness of instructions prohibiting 'borrowing' of tools and equipment

Prevention Measures
- Expectations of strict compliance with policy conveyed to staff by managers, in particular instructions prohibiting the loan of tools and equipment to staff
- Management scrutiny of requisitions - neccessity for purchases/issues to be regularly challenged
- Regular stock-takes of tools and equipment - particularly attractive items
- Results of stock-takes reported to supervisors
- No issues of material, tools and equipment made unless valid job number exists
- Attractive tools and equipment be engraved with identification numbers
- Reports relating to requisitions be produced daily by the stores system and analysed at regular intervals by line managers
- Scrutiny of reports by managers
- Tools and equipment registers maintained
- Asset list and schedule of plant and equipment checked, certified and amended

COMPUTER AND DATA SECURITY

Risks
- Destruction/corruption of data
- Theft of data for commercial purposes
- Unauthorised release of sensitive information
- Theft of equipment

Causes
- Sharing identification numbers and passwords
- Unauthorised access from remote location (hacking)
- Unauthorised access by non-authorised employee
- Security system bypassed
- Poor physical security
- Poor system security
- Abuse of legitimate access
- Viruses etc. or other wilful damage by disgruntled employee or competitor
- Appropriate computer security changes not done when employees with access leave or transfer
- Data files and listings not held under proper security

Prevention Measures
- Appropriate system failures procedure developed and implemented
- Review and investigation of security violation reports
- Computer listings controlled and shredded after use
- Officer not permitted to share identification numbers and passwords
- Regular change of passwords (each 30 days)
- Cancelling access to data when officer transfers or leaves or no longer requires access
- Regular monitoring of users of dial-up facilities
- A sound system of controlling employees with access to data (ie management review of work quality)
- Physical security of equipment and diskettes

INFORMATION AND DISCLOSURES

Risks
- Unauthorised disclosure of sensitive information, whether motivated by personal gain or malice

Causes
- Disgruntled employees
- Information not adequately secured
- Inadequate building security
- No policy governing disclosure
- No classification of information concerning suppliers or contractors
- Pressure from suppliers, contractors or competitors to disclose information
- Employees with prolonged dealings with clients who may seek to corrupt or 'capture' the employees
- Misunderstanding of Freedom of Information obligations
- Lack of computer security

Prevention Measures
- Sensitive material should be identified by managers and classified
- Adequate physical security maintained in respect of sensitive information
- Managers to initiate specific controls/guidelines in sensitive areas and ensure staff compliance:
  - limiting access to confidential information
  - restricting contact to authorised officers

- Managers should ensure that staff in sensitive areas attend fraud awareness training and are made aware of the special procedures in their areas of responsibility
- Sound computer security
- Adequate building security

CONTRACTORS AND CONSULTANTS

Risks
- Bias toward particular contractors
- Disclosure of sensitive information to contractors
- Improper approval in the awarding of contracts
- Biased tender evaluation
- Payment of fraudulent claims
- Kickbacks for biased selection of contractors
- Payments to 'bogus' contractors for false claims
- Bona fides of contractors not checked or deliberately overlooked
- Employees acting as contractors under false names

Causes
- Inducements (eg gifts)
- Inexperienced contract officers
- Too close relationship between officers and contractors resulting in bias or corruption
- Inadequate contract guidelines
- Inadequate segregation of duties
- Poor physical security of sensitive information
- Poor contract management
- Poor supervision
- Poor contract guidelines, policy and procedures

Prevention Measures
- Complete and concise documentation in respect of each contract
- Compliance with policy and procedure
- Guidelines formulated dealing with staff relationships with contractors and consultants
- Training for officers involved in evaluating and administering contracts
- Segregation of duties to exist between advertising, recommending and approval functions
- Exercise of delegations be monitored by supervisory staff
- Managers to monitor compliance with policy and procedures
- Selection criteria developed prior to advertising suspect

For further information on how the Major Fraud Investigation Group can assist you, please contact the:

Major Fraud Investigation Group, Queensland Police Service
200 Roma Street Brisbane Qld 4000

Phone: (07) 3364 6622
Facsimile: (07) 3364 6549

Produced with the assistance of Media & Public Relations Branch
Reproduced from information supplied by the NSW Police Service

Queensland Police Service Vision Statement

We are determined to be a professional police service, dedicated to excellence and committed to working in partnership with the people of Queensland to enhance the safety and security of our community.

FRAUD PREVENTION

GUIDELINES

QUEENSLAND POLICE SERVICE

FRAUD - WHAT IS IT?

Fraud does not always involve the notion of monetary gain, however, it can be defined as encompassing a wide variety of corrupt, deceptive, dishonest or unethical behaviours.

The following definitions have been provided as examples of the average persons understanding of fraud:

"...deceit, trickery, sharp practice or breach of confidence, by which it is sought to gain some unfair or dishonest advantage..."

"...an intentional misstatement of information to obtain financial benefits through improper, unauthorised or illegal actions..."

"...the use of false representations to obtain unjust advantage..."

"...the offence of obtaining money or property by deceit..."

FRAUD RISKS AND PREVENTION INDICATORS

Fraud can flourish in an atmosphere of ignorance and neglect. However, a fraud prevention strategy will assist managers and others to seek out actual and potential fraud, particularly when administrative, managerial and audit failures are exploited by those with fraudulent intent.

The following points should be considered when developing a fraud prevention strategy:

Fraud indicator checklists can be used as an effective tool for reviewing business and organisational performance on a regular basis. Implementation of internal prevention controls is a critical part of the monitoring process for management and improved fraud awareness for employees.

It is also important that businesses and organisations understand the consequences associated with fraud related crime. The following examples of consequences should be noted as examples that occur when fraud prevention/control strategies are not implemented or actively monitored.

- Loss of revenue
- Increased operating expenses
- Reduced operational efficiency
- Inability to meet obligations to employees, suppliers or contractors
- Damage to credibility
- Confidentiality compromised
- Public criticism
- Strategies and plans jeopardised
- Complaints from clients, customers, contractors etc.
- Increased expenditure on salaries, wages and allowances
- Employees encouraged to seek additional loopholes in the award

The following aspects of fraud related crime are common and identify risks, causes and prevention measures.

- Credit Cards
- Cheques
- Salaries, Wages, Overtime Payments
- Materials, Tools, Equipment
- Cash Receipts
- Petty Cash and Advance Accounts
- Purchases and Accounts Payable
- Computer and Data Security
- Information and Disclosures
- Contractors and Consultants

CREDIT CARDS/EFTPOS

Risks

- Fraudulent monetary transactions on credit and debit cards
- Used at bank branches to obtain cash advances
- Used at merchant establishments in payment for goods and/or services
- Used at Automatic Teller Machines (ATMs) to obtain cash advances
- Theft from the authorised holder
- Fraudulent manipulation of EFTPOS terminal by offenders

Causes

- Use of counterfeit credit cards
- Use of stolen/lost credit cards
- Lack of compliance with checking procedures
- Insufficient security of EFTPOS terminal at point of sale
- Often stolen from:
  - The glove boxes of motor vehicles
  - Unattended clothing and handbags in business premises
  - Within the postal system
  - Cardholder letter boxes

Prevention Measures

Check:

- The hologram (inferior and/or different company hologram, three dimensional features, change of colour)
- The commencement date
- The expiry date
- The card is signed
- The signature has not been written over
- The printing and embossing is clean and even for changes to the panel (eg white tape, erasures, smudges)
- Cardholder name and EFTPOS machine receipt details match
- For any visible damage to the card
- Signature on sales strip compared to the actual card
- The signature on receipt
- The card is not returned to the purchaser before sale processed and signature confirmed
- Reverse italics on the signature panel

Detection of alterations or irregularity should be questioned:

- Ask for additional photo identification
- Hold the card
- Call for authorisation
- Request additional account information, eg current balance
- Be aware that card receipts and carbon copies need to be destroyed

Contact the bankcard authorisation centre to obtain authorisation for credit card transactions:

- Where the value of the transaction exceeds the branch/merchant's floor limit
- Where the branch/merchant suspects that the card presenter is not the cardholder
- Check that the refund limit for each EFTPOS terminal is set at an appropriate limit
- Ensure that EFTPOS password or PIN is changed regularly and kept confidential
- Ensure sufficient physical security of EFTPOS terminal

CHEQUES

Risks

- Drawing of uncleared funds from banks, ATMs, EFTPOS
- Fraudulent representation of stolen cheques
- Fraudulent cashing of cheques
- Cheques not met on presentation

Causes

- Inadequate cheque clearance procedures
- Counterfeit bank cheques
- Cheques obtained from companies by persons disguised as repairmen etc and new cheque books ordered from the bank
- Insufficient funds in account for presentation of cheque

Prevention Measures

Make sure that:

- Cheques payable to a third party are properly endorsed by the payee
- Cheque endorsement is in order
- There are no changes on the cheque
- The cheque has the correct date
- Figures match the writing
- Signature is okay
- Contact the company by phone to confirm validity of the cheque
- Contact bank for special clearance of cheque
- Safeguard cheques

CASH RECEIPTS

Risks

- Theft of money

Causes

- Inadequate supervision
- Poor segregation of duties
- Inadequate training of staff
- Use of common registers, drawers etc among staff
- Large amount of cash kept on hand - infrequent banking
- Poor banking procedures
- Poor cash handling and reconciliation procedures

Prevention Measures

- Monitor the number and regularity of 'No Sales' transactions on cash register
- Reduce employees operating with an open cash register
- Cashiers operate their own float and balance when undertaking duties
- Knowledge of safe combination to be limited to only a few people
- Safes to be locked when not in use and located out of public view
- A log book be maintained recording all transactions to and from safes
- Regular depositing of cash receipts into safes
- Daily banking of takings
- Regularly review extent and nature of cash shortages and report instances where satisfactory explanations are not available
- Regularly check bank deposits with cash register totals
- Banking be conducted by two employees

SALARIES, WAGES AND OVERTIME PAYMENTS

Risks

- Fraudulent claims for expenses (eg travelling)
- Fraudulent salaries and wages input documents
- Fraudulent recording of attendance and time
- Fraudulent overtime claims
- Payroll 'ghosts'
- Unnecessary overtime
- Over-award payments

Causes

- Inadequate supervisory review and control
- Claims not properly authorised
- Attendance records not maintained

- Inadequate controls exercised by wages clerks
- Salaries and wages input documents not checked by another officer
- Inexperienced or corrupt wages and salaries clerks
- Employees continue to seek additional loopholes in the award
- Continuing unchallenged long standing practices

Prevention Measures

- Wages clerks should check that allowances are not paid for days absent from work
- Segregation of duties
- Salaries and wages should be randomly checked

PURCHASES AND ACCOUNTS PAYABLE

Risks

- Wasteful expenditure
- Short supply of goods
- Supply of inferior goods
- Payment for services and goods not supplied
- Purchase of goods for private use
- Kickbacks for biased selection of suppliers
- Payments to 'bogus' vendors for false claims
- Cheques written for cash only
- Cheques not properly authorised
- Cost of tyres, repairs, fuel received and paid for by company funds

Causes

- Poor supervisory review
- Systems controls either inadequate or bypassed
- Exercise of delegation not monitored
- Inadequate review of claims for payments
- Inadequate segregation of duties
- Close relationship between employees and suppliers resulting in bias
- Inducements from suppliers (eg gifts)
- Inexperienced purchasing officers inconsistent interpretation
- Improper delegation of authority to personnel to commit, incur and approve expenditure
- No supervisory/independent checks over processing, receipting and payment function for expenditure
- Lack of documentation/information supporting expenditure
- Payment made on photocopies or facsimiles of original invoice

Prevention Measures

- Acknowledgement of receipt of goods and services promptly forwarded
- Quarterly and random audits of petty cash purchases be performed
- At least 10 per cent of daily direct payments (<=$1,000) be checked against appropriate documentation
- Regular follow-up must be maintained by receipting areas of all non-receipted items
- Employees performing accounts payable and stores functions receive appropriate training to ensure compliance with policies
- Segregation of duties to exist between purchasing, receipting and paying functions
- Exercise of delegations be monitored by supervisory staff
- Managers to monitor compliance with policy and procedures
- Ensure expenditure is authorised by a senior officer and is not outside of approved limits/expenditure guidelines
- Ensure that expenditure is supported by required appropriate documentation, ie: original invoice, order number details, original delivery docket
- Ensure that accounts have not been previously paid
- Cheques are not written payable to 'cash'